



PATENT ABSTRACTS OF JAPAN

(11) Publication number: **06162289 A**

(43) Date of publication of application: 10 . 06 . 94

(51) Int. Cl.

G06K 19/10
G06F 15/21
G06K 17/00
G09C 1/00

(21) Application number: **04308688**

(22) Date of filing: 18 . 11 . 92

(71) Applicant: **NIPPON TELEGR & TELEPH
CORP <NTT>**

(72) Inventor: **ISHIGURO GINYA**
MUTA TOSHIYASU
SAKIDA KAZUTAKA

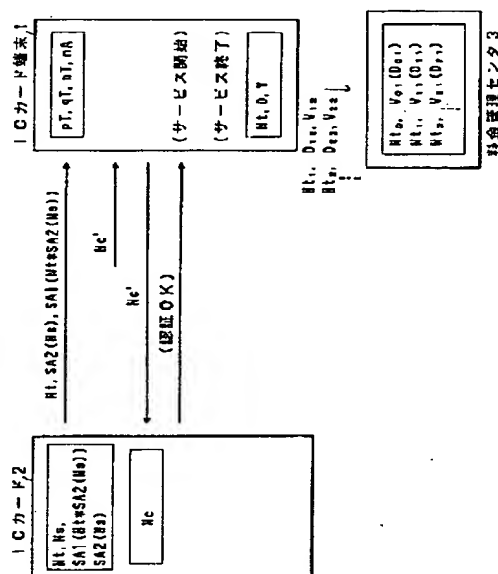
(54) IC CREDIT CARD AND IC CARD TERMINAL

(57) Abstract:

PURPOSE: To dispense with the check of the legality of an user by a center at the time of receiving service.

CONSTITUTION: At the time of issuing an IC card 2, a registration number Nt assigned at every user, a set number Ns for setting a password number use, a digital signature SA2 (Ns) prepared by the master key of an issuer and the digital signature SA1{Nt*SA1(Ns)} prepared by the master key with SA2 (Ns) and Nt are stored in the EEPROM of the IC card 2. At the time of registering the password number Nc, the legality of the user is checked and verified with the IC card 2 by communication with an IC card terminal 1 by Ns known only to the user. By inserting the IC card 2, Nt, SA2 and SA1 are transmitted to the terminal 1 and the terminal 1 verifies SA1 by an open key nA, checks the legality of Nt and when it is correct, let the password number be inputted. When the user inputs Nc', the IC card 2 compares it with Nc of the inside and transmits authentication to the terminal 1 in the case of coincidence and when it is received, the terminal 1 permits the user to receive the service.

COPYRIGHT: (C)1994,JPO&Japio



Best Available Copy

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開平6-162289

(43)公開日 平成 6年(1994) 6月10日

(51)Int.Cl. ⁵	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 K 19/10				
G 0 6 F 15/21	3 4 0 B	7052-5L		
G 0 6 K 17/00	T	7459-5L		
G 0 9 C 1/00		8837-5L		
		8623-5L		
			G 0 6 K 19/ 00	R
			審査請求 未請求	請求項の数 2 (全 10 頁)

(21)出願番号 特願平4-308688

(22)出願日 平成 4年(1992)11月18日

(71)出願人 000004226

日本電信電話株式会社

東京都千代田区内幸町一丁目 1 番 6 号

(72)発明者 石黒 銀矢

東京都千代田区内幸町 1 丁目 1 番 6 号 日

本電信電話株式会社内

(72)発明者 牟田 敏保

東京都千代田区内幸町 1 丁目 1 番 6 号 日

本電信電話株式会社内

(72)発明者 崎田 一貴

東京都千代田区内幸町 1 丁目 1 番 6 号 日

本電信電話株式会社内

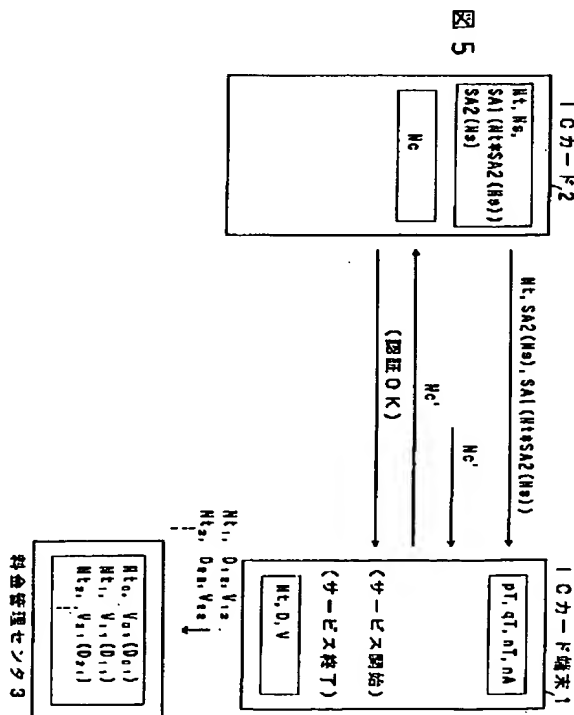
(74)代理人 弁理士 草野 卓

(54)【発明の名称】 ICクレジットカード及びICカード端末

(57)【要約】 (修正有)

【目的】 サービスを受けるに当りセンタによる利用者の正当性のチェックの不要化。

【構成】 ICカード2発行の際、利用者ごとに割付けられた登録番号N tと、暗証番号設定用設定番号N sと、発行者のマスタ鍵でN sに作成したデジタル署名S A 2 (N s)と、S A 2 (N s)とN tにマスタ鍵で作成したデジタル署名S A 1 (N t * S A 1 (N s))とをICカード2のEEPROMに記憶しておく。暗証番号N c登録の際は、利用者しか知らないN sで利用者の正当性をICカード端末1とのやりとりでICカード2でチェック検証する。ICカード2の挿入で、N t、S A 2、S A 1が端末1へ送られ、端末1は公開鍵n AでS A 1を検証し、N tの正当性をチェックし、正しければ暗証番号を入力させる。利用者のN c' 入力で、ICカード2は内部のN cと比較し、一致すれば認証化を端末1へ送り端末1はこれを受けると利用者にサービスを受けることを許す。



1

【特許請求の範囲】

【請求項1】 利用者を特定するための登録番号N t、暗証番号を設定するための設定番号N s、前記登録番号N tを含む情報に対するマスタ鍵によるデジタル署名S Aを記録するとともに、暗証番号N cを記録するためのメモリと、

前記登録番号N t、前記デジタル署名S AをICカード端末へ送信する手段と、

前記ICカード端末から受信した設定番号N s' と前記メモリに記録している設定番号N s との比較を行い、一致したとき第1の認証通知を前記ICカード端末へ送信する手段と、

暗証番号登録時に、前記ICカード端末から暗証番号N c、その暗証番号N cを含む情報に対する前記ICカード端末によるデジタル署名S T、前記ICカード端末の端末公開鍵n Tを受信し、前記受信したデジタル署名S Tを受信した端末公開鍵n Tで検証し、正しい場合にのみ前記メモリに受信した暗証番号N cを記録する手段と、

サービス開始前に、前記ICカード端末から受信した暗証番号N c' と前記メモリに記録している暗証番号N c との比較を行い、一致したとき第2の認証通知を前記ICカード端末へ送信する手段と、

を具備するICクレジットカード。

【請求項2】 デジタル署名S Aを検証するためのマスタ公開鍵n A及び端末公開鍵n T、デジタル署名をするための端末鍵p T、q Tを記録したメモリと、

ICカードから受信したデジタル署名S Aを前記公開鍵n Aで検証し、受信した登録番号N tが正しければ暗証番号の登録または暗証番号の入力を許可する手段と、暗証番号の登録が選択されたとき、入力手段から入力された登録番号N t' と受信した登録番号N t との比較を行い、一致したとき設定番号の入力を指示する手段と、前記入力手段から入力された設定番号N s' を前記ICカードへ送信する手段と、

前記ICカードから第1の認証通知を受信したとき、前記入力手段から入力された暗証番号N cを含む情報に対して前記端末鍵p T、q Tを用いてデジタル署名S Tを作成する手段と、

前記暗証番号N c、前記デジタル署名S T、前記端末公開鍵n Tを前記ICカードに送信する手段と、

暗証番号の入力が選択されたとき、前記入力手段から入力された暗証番号N c' を前記ICカードに送信する手段と、

前記ICカードから第2の認証通知を受信したとき、サービスを許可する手段と、

を具備したICカード端末。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 この発明は、あらかじめ登録番号

2

などを登録してあるICカードをICカード端末へ利用者が挿入することによりサービスの提供を受け、そのサービスについて後に料金の請求を受けるようにしたICクレジットカードシステムに用いられる前記ICクレジットカード及び前記ICカード端末に関する。

【0002】

【従来の技術】 従来のICクレジットカードシステムは、サービス提供前に、ICカード端末と、登録番号などを登録しているセンタとをオンラインでつなぎ、利用者がダイヤル操作により登録番号などを入力し、入力された情報がセンタに送られ、センタであらかじめ登録されている利用者情報により利用者の正当性のチェックが行われ、正当であることが確認されたとき、ICカード端末でのサービスの提供を可能としていた。

【0003】

【発明が解決しようとする課題】 したがって、従来においては、サービス提供前にセンタとICカード端末とが通信を行う必要があり、オンラインで検証を行うためにセンタ設備が大規模になったり、通信料がサービス提供料金の他に必要になるなど欠点があった。

【0004】

【課題を解決するための手段】 この発明によるICクレジットカードは、利用者を特定するための登録番号N t、暗証番号を設定するための設定番号N s、前記登録番号N tを含む情報に対するマスタ鍵によるデジタル署名S Aを記録するとともに、暗証番号N cを記録するためのメモリと、前記登録番号N t、前記デジタル署名S AをICカード端末へ送信する手段と、前記ICカード端末から受信した設定番号N s' と前記メモリに記録している設定番号N s との比較を行い、一致したとき第1の認証通知を前記ICカード端末へ送信する手段と、暗証番号登録時に、前記ICカード端末から暗証番号N c、前記暗証番号を含む情報に対する前記ICカード端末によるデジタル署名S T、前記ICカード端末の端末公開鍵n Tを受信し、その受信したデジタル署名S Tを前記端末公開鍵n Tで検証し、正しい場合にのみ前記メモリに受信した暗証番号N cを記録する手段と、サービス開始前に、前記ICカード端末から受信した暗証番号N c' と前記メモリに記録している暗証番号N c との比較を行い、一致したとき第2の認証通知を前記ICカード端末へ送信する手段とを具備する。

【0005】 この発明によるICカード端末は、デジタル署名S Aを検証するためのマスタ公開鍵n A及び端末公開鍵n T、デジタル署名をするための端末鍵p T、q Tを記録したメモリと、受信したデジタル署名S Aを前記公開鍵n Aで検証し、受信した登録番号N tが正しければ暗証番号の登録または暗証番号の入力を許可する手段と、暗証番号の登録が選択されたとき、入力手段から入力された登録番号N t' と受信した登録番号N t との比較を行い、一致したとき設定番号の入力を指示する手

段と、入力手段から入力された設定番号 Ns' をICカードへ送信する手段と、前記ICカードから第1の認証通知を受信したとき、入力手段から入力された暗証番号 Nc を含む情報に対して前記端末鍵 pT 、 qT を用いてデジタル署名 ST を作成する手段と、前記暗証番号 Nc 、前記デジタル署名 ST 、前記端末公開鍵 nT を前記ICカードに送信する手段と、暗証番号の入力が選択されたとき、入力手段から入力された暗証番号 Nc' を前記ICカードに送信する手段と、前記ICカードから第2の認証通知を受信したとき、サービスを許可する手段とを具備する。

【0006】

【作用】このような構成のICクレジットカード（以下単にICカードと記す）、ICカード端末を設ければ、デジタル署名付きの登録番号によってICカードの正当性をICカード端末で検証できるとともに、利用者が入力した暗証番号により、利用者の正当性をICカードで検証でき、さらに暗証番号の登録時には利用者しか知り得ない設定番号により利用者の正当性をICカードで検証できるので利用者の情報に関するデータベースを持つセンタへサービス開始前にアクセスする必要がなく、しかも不正なICカードによるサービス利用も排除することができる。

【0007】

【実施例】次に図を参照にして請求項1及び2の発明の各実施例を説明する。図1は、この発明のICカード及びICカード端末が適用されるICクレジットカードシステム構成例を示す。ICカード端末1はICカード2により検証処理を行い、通話など各種サービスを提供する。料金管理センタ3はICカード2により利用したサービス料金を管理する。ICカード端末1は利用されたICカード2の登録番号と利用料金をメモリに蓄えておき、適当な間隔、例えば日ごとに料金管理センタ3へ自動的に発信し、蓄えた情報を料金管理センタ3へ通信網4を介して送信する。料金管理センタ3では登録番号ごとに利用料金を集計し、例えば月ごとに利用者へ利用料金の請求を行う。

【0008】図2はICカード端末1の内部構成を示す図であり、制御部11は処理手順などのプログラムを内部のROMに記録しているとともに、鍵情報などを内部RAMに記録している。鍵情報などは、ICカード端末設置時に、通信網を介してセンタ装置（図示せず）と接続し、センタ装置から受信してRAMに記録してもよく、ICカード端末製造時に予め設定してもよい。ICカード2とデータのやりとりを行うICカードリーダライタ部12、暗証番号の登録を指示する操作ボタン、ダイヤルボタンなどからなる操作入力部13、液晶ディスプレイからなる表示部14及び通話回路15が制御部11に接続され、通話回路15に送受器16が接続されまた通信網との処理を行う通信処理部17が制御部11に

接続されている。

【0009】図3はICカード2の内部構成を示す図であり、ICカードの処理手順等のプログラムはROM61に記憶され、CPU63はワークエリアとしてRAM62を利用してすべての制御を行い、図2に示したICカード端末1のICカードリーダライタ部12との通信は通信部65により接点66を介して行われる。登録番号、設定番号、デジタル署名はICカード2の発行時にICカード発行機（図示せず）によって書き込まれEEPROM64に記録されている。

【0010】図4は利用者がICカード端末1を使ってICカード2に暗証番号を登録する操作を説明する図である。ICカード2のEEPROM64の所定エリアに、利用者を特定するための登録番号 Nt 、暗証番号を設定するために利用者ごとに割り付けられた設定番号 Ns 、その設定番号 Ns に対して発行者がマスタ鍵によって作成した第2のデジタル署名 $SA2(Ns)$ 、登録番号 Nt および第2のデジタル署名 $SA2(Ns)$ に対して発行者がマスタ鍵によって作成した第1のデジタル署名 $SA1(Nt * SA2(Ns))$ が記録されている。この記録の際に第2のデジタル署名 $SA2(Ns)$ を公開鍵 nA で検証して設定番号 Ns の正当性を判断することができる。また、ICカード端末1の制御部11内のRAMの所定のエリアに、前記マスタ鍵によって作成されたデジタル署名を検証するためのマスタ公開鍵 nA 、ICカードが端末がデジタル署名を作成するための端末鍵 pT 、 qT 、前記ICカード端末が作成したデジタル署名を検証するための端末公開鍵 nT が記録されている。デジタル署名としては、例えば「NTT R&D Vol.40 No.5 P. 687~696 (1991)」に掲載されているESIGNを使用することができる。

【0011】利用者がICカード2をICカード端末1のICカードリーダライタ部12に挿入すると、ICカード2からICカード端末1に登録番号 Nt 、第2のデジタル署名 $SA2(Ns)$ 、第1のデジタル番号 $SA1(Nt * SA2(Ns))$ が送信される。ICカード端末1はマスタ公開鍵 nA により第1のデジタル署名 $SA1$ の検証を行い、 Nt の正当性を判断する。この場合第2のデジタル署名 $SA2$ の検証も行い、これの正当性も判断すると一そう正確になる。正当でないと判断した場合にはICカードを返却して処理を中止する。両者とも正当であると判断した場合には“暗証番号の入力”を指示する画面を表示部14に表示する。この画面が表示されている間は、暗証番号の入力を可能とするとともに、操作入力部13のボタン操作による暗証番号の登録を有効とする。ここで、暗証番号を入力してもICカード2に暗証番号が登録されていなければ暗証番号不一致として処理される。操作入力部13の暗証番号登録ボタンを押すことにより暗証番号登録処理に移行する。ICカード2へ暗証番号登録通知を送信し、ICカード2へ暗証

番号登録処理に入ったことを知らせるとともに、表示部 14 に“登録番号をダイヤルしてください”と表示し、利用者に登録番号の入力を促す。利用者がダイヤルにより登録番号 N_t' を入力すると、ICカード端末 1 は先に ICカード 2 から受信した登録番号 N_t との比較を行い、利用者が入力した番号の正当性をチェックする。一致しない場合には再度登録番号の入力を促すが、例えば 3 回の入力後も一致しない場合には、不正使用と判断し ICカード 2 を返却して処理を中止する。一致した場合には表示部 14 に“設定番号をダイヤルしてください”と表示し、利用者に設定番号の入力を促す。

【0012】利用者がダイヤルにより設定番号 N_s' を入力すると、ICカード端末 1 は ICカード 2 へ設定番号 N_s' を送信する。ICカード 2 は受信した設定番号 N_s' と前記メモリに予め記録している設定番号 N_s との比較を行い、利用者が入力した設定番号の正当性をチェックする。一致しない場合には ICカード端末 1 へ不一致通知を送信し、ICカード端末 1 は再度設定番号の入力を促すが、例えば 3 回の入力後も一致しない場合には、不正使用と判断し ICカード 2 を返却して処理を中止する。一致した場合には ICカード 2 は認証 OK (第 1 の認証通知) を ICカード端末 1 へ送信する。ICカード端末 1 は表示部 14 に“暗証番号をダイヤルしてください”と表示し、利用者に暗証番号の入力を促す。利用者がダイヤルにより暗証番号 N_c を入力すると、ICカード端末 1 は暗証番号 N_c に対して端末鍵 p_T 、 q_T によるデジタル署名 $ST(N_c)$ を作成し、ICカード 2 に暗証番号 N_c とともにデジタル署名 $ST(N_c)$ および端末公開鍵 n_T を送信する。ICカード 2 は端末公開鍵 n_T によりデジタル署名 $ST(N_c)$ の検証を行い、暗証番号 N_c の正当性のチェックを行う。正当であることが検証できた場合には暗証番号 N_c を RAM62 に記録する。

【0013】上記の処理において、設定番号 N_s の検証を ICカード 2 で行うようにしているが、最初に登録番号 N_t を ICカード端末 1 へ送信するときに設定番号 N_s もいっしょに送信しておけば ICカード端末 1 で設定番号のチェックを行うことができる。ただし、この場合には設定番号 N_s という他人には知られてはならない情報が ICカード 2 から送信されるためセキュリティという面からは好ましくない。また、登録番号あるいは設定番号のダイヤル時に、3 回の入力後も一致しない場合には、不正カードである旨を ICカード 2 に記録することにより、以降その ICカードの使用を不能とすることもできる。

【0014】図 5 は利用者が ICカード 2 を使って ICカード端末 1 からサービスを受けるときの処理を説明する図である。ICカード 2 の RAM62 には暗証番号 N_c が記録されている。利用者が ICカード 2 を ICカード端末 1 の ICカードリーダーライタ部 12 に挿入する

と、ICカード 2 から ICカード端末 1 に登録番号 N_t 、第 2 のデジタル署名 $SA_2(N_s)$ 、第 1 のデジタル署名 $SA_1(N_t * SA_2(N_s))$ が送信される。ICカード端末 1 はマスタ公開鍵 n_A によりデジタル署名 SA_1 の検証を行い、登録番号 N_t の正当性を判断する。この場合も第 2 のデジタル署名の正当性を判断した方がよい。正当でないと判断した場合には ICカード 2 を返却し処理を中止する。正当であると判断した場合には“暗証番号の入力”を指示する画面を表示部 14 に表示する。この画面が表示されている間は、暗証番号の入力を可能とするとともに、操作入力部 13 のボタン操作による暗証番号の再登録も有効である。つまり暗証番号を変更することもできる。ここで、利用者が暗証番号 N_c' をダイヤルすると、この N_c' は ICカード 2 へ送信され、ICカード 2 内でその内部に記録してある暗証番号 N_c との比較が行われる。一致しない場合には ICカード 2 から ICカード端末 1 へ認証不一致通知が送信され、ICカード端末 1 は再度暗証番号の入力を促す。例えば 3 回の入力後も一致しない場合には、不正使用と判断して ICカード 2 を返却して処理を中止する。

【0015】一致した場合には ICカード 2 は認証 OK (第 2 の認証通知) を ICカード端末 1 へ送信する。ICカード端末 1 は、所定のサービスが可能であることを表示部 14 に表示し、所定のサービスを実行する。例えば通常の通話サービスであれば、相手の番号がダイヤルできる旨を表示し、利用者のダイヤルした相手に接続する。これにより通話サービスを受けることができ、利用者がそのサービス利用を終了すると、ICカード端末 1 はその利用者を特定する登録番号 N_t 、利用日時 D 、利用料金 V を内部のメモリに記録し、ICカード 2 を排出して処理を終了する。その内部のメモリに蓄えたデータは、例えば 1 日に一回程度の割合で料金管理センタ 3 に送信する。料金管理センタ 3 ではこれを受信して登録番号ごとに料金を集計し、毎月利用者に請求書を送付して料金の支払いを受ける。

【0016】図 6 はこの発明の他の実施例を示し、利用者が ICカード端末 1 を使って ICカード 2 に暗証番号を登録する操作を説明する図である。ICカード 2 の EPROM64 には N_t 、 N_s 、 $SA_2(N_s)$ 、 $SA_1(N_t * SA_2(N_s))$ が記録されている他に、ICカード 2 がデジタル署名を作成するためのカード鍵 p_U および q_U 、ICカードが作成したデジタル署名を検証するためのカード公開鍵 n_U も記録されている。また、ICカード 2 および ICカード端末 1 は各々乱数生成用のプログラムをメモリに記録している。暗証番号の登録処理において、前述した手順により登録番号、設定番号の検証を終え、利用者がダイヤルボタンから暗証番号 N_c を入力すると、ICカード端末 1 は乱数 R を生成し、ICカード 2 へ乱数 R を送信する。ICカード 2 は乱数 X を生成し、受信した乱数 R および生成した乱数 X

に対してカード鍵 pU 、 qU を用いてデジタル署名 $SU(R * X)$ を作成し、作成したデジタル署名 $SU(R * X)$ とともに乱数 X およびカード公開鍵 nU をICカード端末1へ送信する。

【0017】ICカード端末1は受信したカード公開鍵 nU により受信したデジタル署名 SU を検証し、ICカード2が正当な相手であることを認証する。正当な相手であることを認証すると、乱数 R および X 、暗証番号 Nc に対して端末鍵 pT 、 qT によりデジタル署名 $ST(R * X * Nc)$ を作成し、作成したデジタル署名 $ST(R * X * Nc)$ とともに端末公開鍵 nT 、暗証番号 Nc をICカード2へ送信する。ICカード2は受信した端末公開鍵 nT によりデジタル署名 ST を検証し、ICカード端末1が正当な相手であることを認証するとともに暗証番号の正当性を認証し、暗証番号 Nc をRAM62に記録する。この実施例の場合には情報の送受に相互に生成した乱数を使用しているため信号の内容が同一になることがなく、傍受した信号を利用した不正を防止することができる。また、相互にデジタル署名を作成して相互認証を行っているためセキュリティをより高めることができる。

【0018】図7はこの発明の他の実施例を示し、図6で説明したICカード2およびICカード端末1によりサービスを受けるときの処理を説明する図である。利用者がICカード2をICカード端末1へ挿入し、図5で前述した手順により登録番号の検証を終え、利用者がダイヤルボタンから暗証番号 Nc' を入力すると、ICカード端末1は乱数 R を生成し、ICカード2へ乱数 R 、及び暗証番号 Nc' を送信する。ICカード2は受信した暗証番号 Nc' とメモリに記録している暗証番号 Nc との比較を行い、一致していれば乱数 X を生成し、受信した乱数 R および生成した乱数 X に対してカード鍵 pU 、 qU によりデジタル署名 $SU(R * X)$ を作成し、その作成したデジタル署名 $SU(R * X)$ とともに乱数 X およびカード公開鍵 nU をICカード端末1へ送信する。ICカード端末1は受信したカード公開鍵 nU により受信したデジタル署名 SU を検証し、ICカード2が正当な相手であることを認証するとともに暗証番号が正当であると判断し、所定のサービスが可能であることを表示部14に表示し、所定のサービスを実行する。サービスが終了すると、利用者を特定する登録番号 Nt 、利用日時 D 、利用料金 V を内部のメモリに記録し、ICカード2を排出して処理を終了する。

【0019】上記の説明において、ICカード2を特定するカード番号 IDU と、カード番号に対して発行者がマスタ鍵により作成したデジタル署名 $SA(IDU)$ とをICカード2の発行時にEEPROM64に記録しておき、ICカード2をICカード端末1に挿入したとき、登録番号 Nt とともにカード番号 IDU 、デジタル署名 $SA(IDU)$ を送信し、マスタ公開鍵によってS

Aを検証することによりカード番号の正当性をチェックするように構成すれば、ICカード2の紛失などに対処することができる。すなわち、ICカード2を紛失したときに利用者が発行者に申告することにより、発行者はICカード2のカード番号をダウンロードによりICカード端末1にブラックリストとして登録する。ICカード端末1はICカード2が挿入されたときカード番号 IDU とブラックリストとを比較する。一致するICカードがあった場合にはそのICカードの使用を制限することができる。

【0020】また、ICカード2のEEPROM64に日付情報を記録しておき、ICカード2をICカード端末1に挿入したとき、登録番号とともに日付情報を送信し、ICカード端末1に内蔵したカレンダーと比較することによりICカード2の使用可否を判断するように構成すれば有効期限付きのICカード2とすることができる。

【0021】さらに、ICカード2およびICカード端末1に送信情報の暗号化のためのアルゴリズムと暗号化および復号化のための共通の鍵をメモリに記録しておくことにより、相互の通信を暗号通信により行うことができ、よりセキュリティを高めることができる。

【0022】

【発明の効果】この発明によるICカードとICカード端末とを用いられれば、ICカードとICカード端末との間で相互の正当性を検証することになり、かつ利用者の正当性を、ICカード端末を介してICカードで検証するようになり、サービスの利用時あるいは暗証番号の設定時に利用者の情報に関するデータベースを持つセンタへアクセスする必要がなく、容易にシステムを構築することができる。また、センタへアクセスする必要がないため検証時間も短縮でき、操作性にすぐれたシステムとなる。さらに、発行者しか知り得ないマスタ鍵によるデジタル署名により登録番号の検証を行うように構成しているため、例え他人の登録番号を知り得てもデジタル署名を作成することはできず、また、拾ったICカードでは暗証番号が分からず、登録番号、設定番号が不明なため暗証番号を変更することも不可能でありセキュリティの高いシステムを構築することができる。

【図面の簡単な説明】

【図1】この発明のICカード、ICカード端末を使用してICクレジットカードシステムを構成した例を示すブロック図。

【図2】この発明によるICカード端末の構成例を示すブロック図。

【図3】この発明によるICカードの構成例を示すブロック図。

【図4】この発明によるICカードとICカード端末とを用いて、ICカードに暗証番号を登録する場合の処理手順を示す図。

【図 5】図 4 で示した手法で登録された暗証番号の I C カードによりサービスを受ける場合の処理手順を示す図。

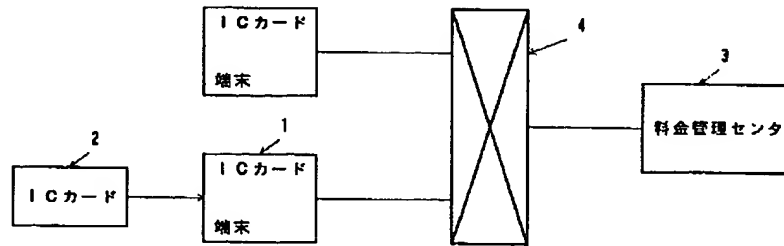
【図 6】この発明の他の実施例により暗証番号を登録す*

*る場合の処理手順を示す図。

【図 7】図 6 で示した手順で登録された暗証番号の I C カードによりサービスを受ける場合の処理手順を示す図。

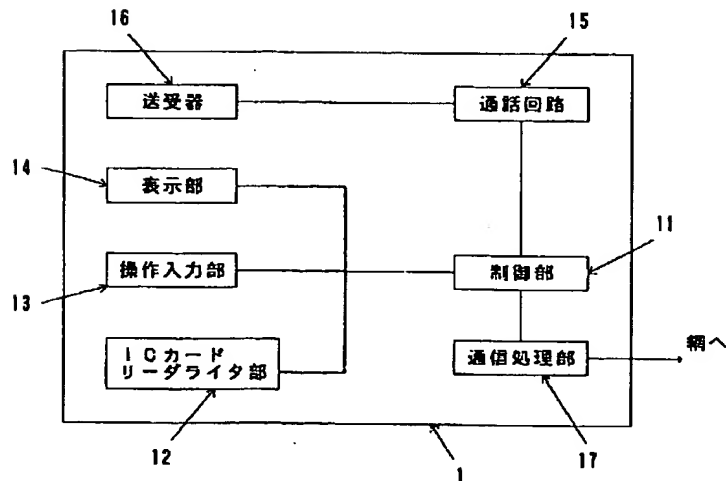
【図 1】

図 1



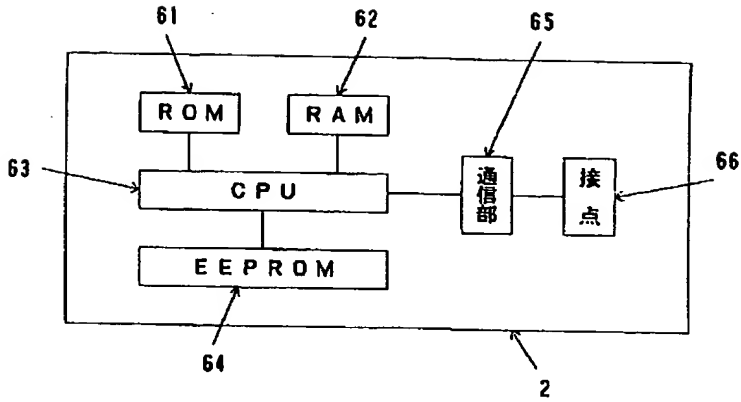
【図 2】

図 2



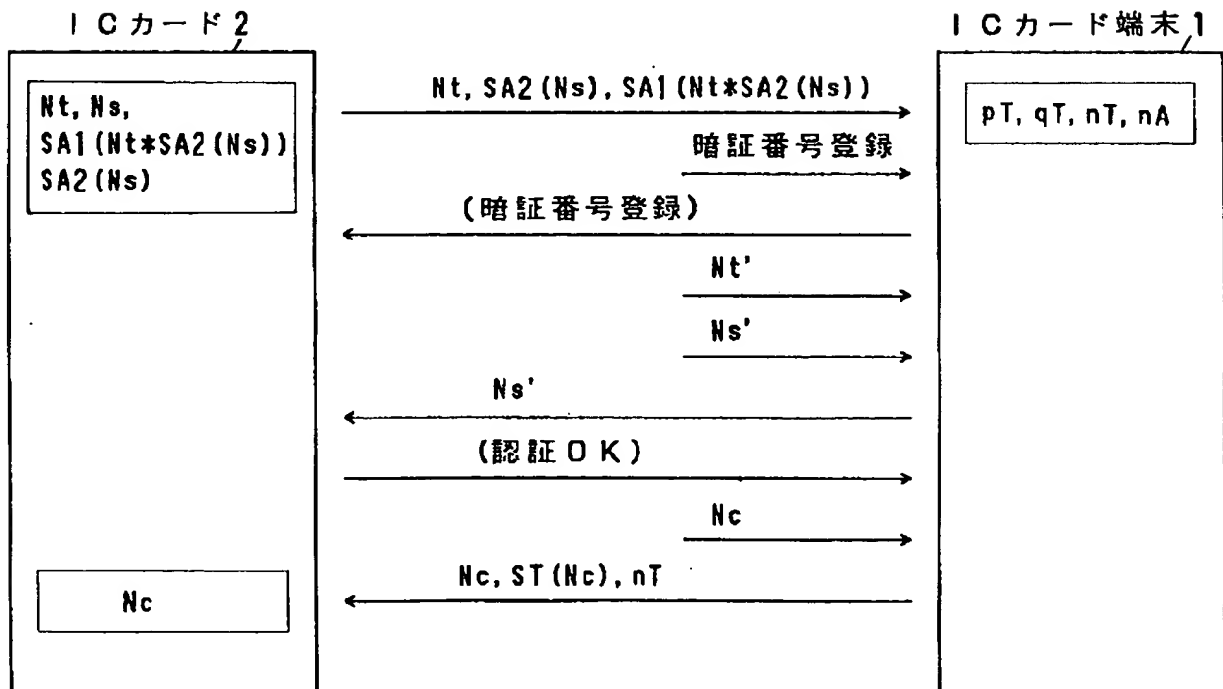
【図3】

図 3



【図4】

図 4



【図5】

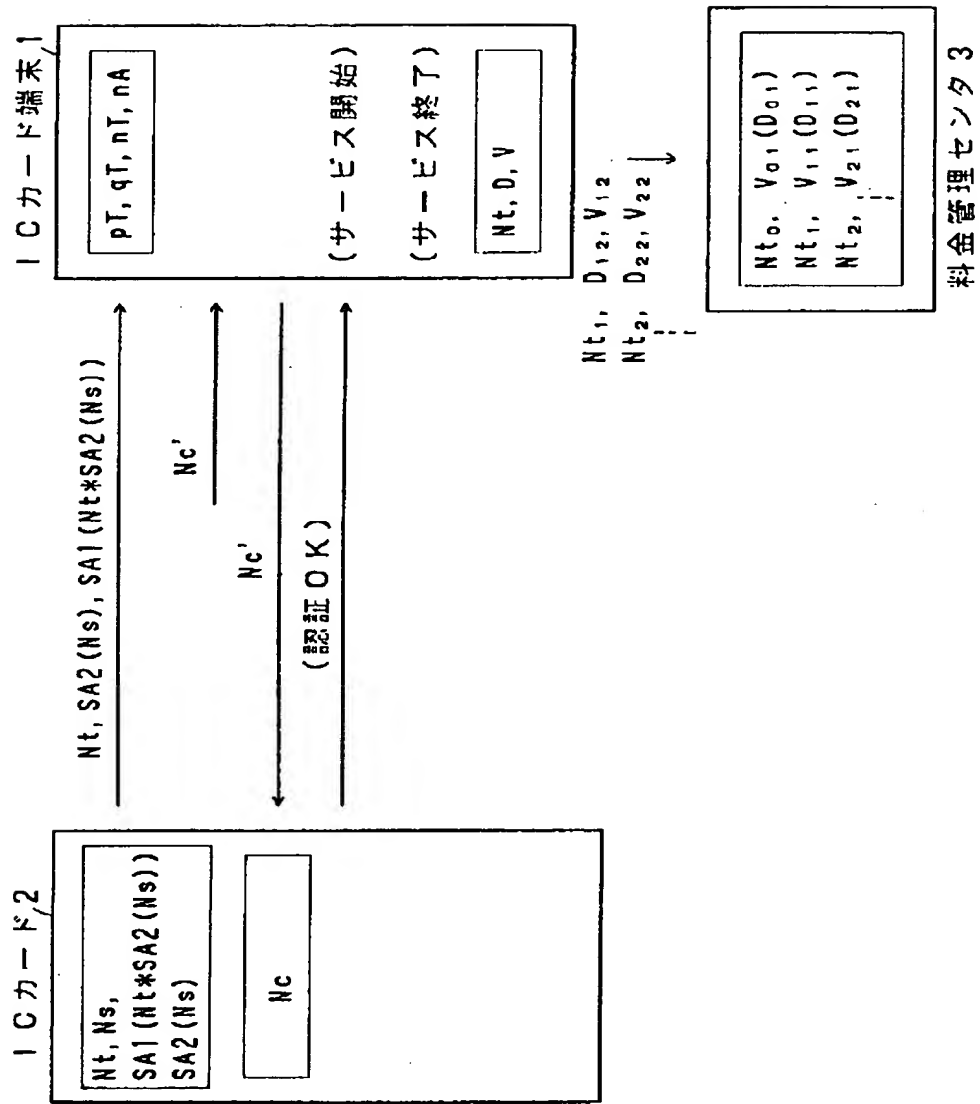
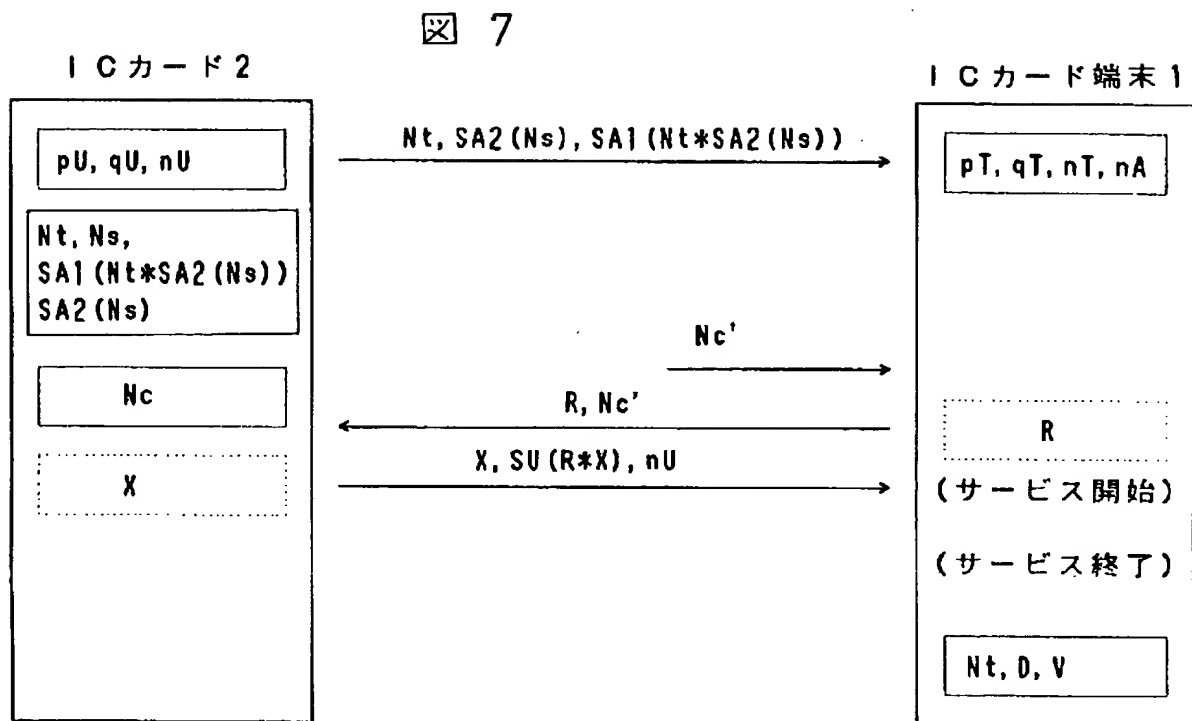


図5

【図7】



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.